Sub B2 >

~~CLAIMS~~

Sub B3 >

1. A data recording/reproducing method wherein encrypted digital data obtained by subjecting digital data to first encrypting by using a contents key and encrypted contents key obtained by subjecting said contents key to second encrypting are recorded on a recording medium, said encrypted digital data and said encrypted contents key, having been recorded, are reproduced, and said encrypted digital data is decrypted by using said contents key obtained by decrypting said encrypted contents key, thereby to obtain said digital data.

2. A data recording/reproducing method in accordance with claim 1, wherein said encrypted contents key is recorded in a data area on said recording medium, from which data is output outside.

3. A data recording/reproducing method in accordance with claim 1 or 2, wherein said contents key is switched at regular or irregular intervals.

4. A data recording/reproducing system comprising a contents encrypting means for receiving digital data and a contents key for encrypting said digital data and for subjecting said digital data to first encrypting by using said contents key to generate encrypted digital data, a key encrypting means for subjecting said contents key to second encrypting to generate a encrypted contents key, a recording

means for recording said encrypted digital data and said encrypted contents key on a recording medium, a reproducing means for reproducing said encrypted digital data and said encrypted contents key from said recording medium, a key decrypting means for decrypting said encrypted contents key to restore said contents key, and a contents decrypting means for decrypting said encrypted digital data by using said contents key to obtain said digital data.

5. A data recording/reproducing system in accordance with claim 4, wherein all of said means are provided for an integrated apparatus.

6. A data recording/reproducing system in accordance with claim 4, wherein said receiving means, said contents encrypting means and said contents decrypting means are provided for a tuner apparatus, and said recording means and said reproducing means are provided for a VTR apparatus.

7. A data recording/reproducing system in accordance with claim 6, wherein said second encrypting is carried out by using a public key, and said encrypted contents key is decrypted by using a secret key corresponding to said public key.

8. A data recording/reproducing system in accordance with claim 7, wherein said key decrypting means is provided for said tuner apparatus.

9. A data recording/reproducing system in accordance

with claim 8, wherein said public key and said secret key are keys inherent in said tuner apparatus.

10. A data recording/reproducing system in accordance with claim 8, wherein said public key and said secret key are keys inherent in the device model of said tuner apparatus.

11. A data recording/reproducing system in accordance with claim 8, wherein said tuner apparatus has a card reading means capable of reading information recorded on an IC card.

12. A data recording/reproducing system in accordance with claim 11, wherein said public key and said secret key are keys inherent in the user ID recorded on said IC card.

13. A data recording/reproducing system in accordance with claim 11, wherein said public key and said secret key are keys inherent in the service recorded on said IC card.

14. A data recording/reproducing system in accordance with claim 12, wherein in addition to said key inherent in said user ID, a public key inherent in at least another user ID is recorded on said IC card, said key encrypting means encrypts said contents key by using said public key inherent in said other user ID, in addition to said second encrypting, thereby to generate another encrypted contents key for each public key inherent in said other user ID, and said recording means records said other encrypted contents key, in addition to said encrypted contents key.

15. A data recording/reproducing system in accordance with one of claims 8 to 14, wherein said key encrypting means is provided for said tuner apparatus or said VTR apparatus.

16. A data recording/reproducing system in accordance with claim 15, wherein, in the case when said key encrypting means is provided for said VTR apparatus, said tuner apparatus has a second key encrypting means for encrypting said contents key by using a common key, and said VTR apparatus has a second key decrypting means for decrypting said contents key encrypted by using said common key.

17. A data recording/reproducing system in accordance with claim 7, wherein said public key and said secret key are keys inherent in said VTR apparatus, and said key encrypting means and said key decrypting means are provided for said VTR apparatus.

18. A data recording/reproducing system in accordance with claim 17, wherein said tuner apparatus has a second key encrypting means for encrypting said contents key by using a common key and a second key decrypting means for decrypting said contents key encrypted by using said common key, said VTR apparatus has a third key encrypting means for encrypting said contents key by using said common key and a third key decrypting means for decrypting said contents key encrypted by using said common key, said third key decrypting means decrypts said contents key encrypted by

said second key encrypting means, and said second key decrypting means decrypts said contents key encrypted by said third second key encrypting means.

19. A data recording/reproducing system in accordance with claim 6, wherein said second encrypting and said decrypting of said encrypted contents key are executed by using a common key, and said key encrypting means and said key decrypting means are provided for said tuner apparatus.

20. A data recording/reproducing system in accordance with claim 19, wherein said common key is inherent in said tuner apparatus or the device model of said tuner apparatus.

21. A data recording/reproducing system in accordance with claim 19, wherein said tuner apparatus has a card reading means capable of reading information recorded on an IC card, and said common key is inherent in the user ID recorded on said IC card or the service recorded on said IC card.

22. A data recording/reproducing system in accordance with one of claims 6 to 21, wherein said tuner apparatus generates and stores billing information at the time of recording by said recording medium.

23. A data recording/reproducing system in accordance with one of claims 6 to 21, wherein said tuner apparatus generates and stores billing information at the time of reproduction by said recording medium.

24. A data recording/reproducing system in accordance with claim 23, wherein information required to generate said billing information is recorded on said recording medium at the time of recording by said recording medium, and said billing information is generated by using said required information at the time of reproduction by said recording medium.

25. A data recording/reproducing system in accordance with claim 23 or 24, wherein the billing information is provided with limitation of the reproduction period of said recording medium.

26. A data recording/reproducing system in accordance with one of claims 23 to 25, wherein the billing information is provided with limitation of the number of reproductions of said recording medium.

27. A data recording/reproducing system in accordance with one of claims 22 to 26, wherein said tuner apparatus stores said billing information on said IC card.

28. A data recording/reproducing system in accordance with one of claims 22 to 27, wherein said tuner apparatus outputs said billing information to a service provider via communications.

29. A data recording/reproducing system in accordance with one of claims 4 to 28, wherein said encrypted contents key is recorded in a data area on said recording medium,

from which data is output outside.

30. A data recording/reproducing system in accordance with one of claims 4 to 29, wherein information regarding the inherence of said key subjected to said second encrypting is stored on said recording medium.

31. A data recording/reproducing system in accordance with one of claims 4 to 30, wherein said contents key is switched at regular or irregular intervals.

32. A data recording/reproducing system in accordance with claim 31, wherein said recording medium is reproduced so that said encrypted contents key corresponding to said contents key after switching overlaps at least a part of said encrypted digital data corresponding to said contents key before switching with respect to timing.

33. A data recording/reproducing system in accordance with claim 31 or 32, wherein said recording medium is reproduced so that said encrypted contents key corresponding to one of said contents keys overlaps said encrypted digital data corresponding thereto with respect to timing.

34. A data recording/reproducing system in accordance with one of claims 31 to 33, wherein, in the case when said tuner apparatus is provided, said tuner apparatus carries out said switching.

35. A data recording/reproducing system in accordance

with one of claims 31 to 34, wherein, in the case when said VTR is provided, said VTR apparatus determines the reproduction timing of said encrypted contents key in response to said switching.

36. A data recording/reproducing system in accordance with one of claims 31 to 35, wherein said encrypted digital data and said encrypted contents key are recorded at the recording position corresponding to said reproduction timing on said recording medium.

37. A data recording/reproducing system in accordance with claim 36, wherein said switching timing is also recorded on said recording medium.

38. A data recording/reproducing system in accordance with one of claims 31 to 37, wherein, in the case when said tuner apparatus and said VTR are provided, said VTR apparatus outputs said contents key for use after switching or said encrypted contents key corresponding thereto to said tuner apparatus, before outputting said encrypted digital data corresponding to said contents key for use after switching.

39. A recording apparatus comprising:

a contents encrypting means for receiving digital data and a contents key for encrypting said digital data and for subjecting said digital data to first encrypting by using said contents key to generate encrypted digital data,

a key-encrypting key generating means for generating

a key-encrypting key for subjecting said contents key to second encrypting,

a storing means for storing said key-encrypting key and for deleting said key-encrypting key hereafter if said key-encrypting key satisfies a predetermined condition,

a key encrypting means for generating a encrypted contents key by subjecting said contents key to said second encrypting by using said key-encrypting key,

a relationship information generating means for generating the relationship information between said encrypted digital data encrypted by using said contents key and said key-encrypting key obtained by encrypting said contents key, and

a recording means for receiving said encrypted digital data, said encrypted contents key and all or part of said relationship information and for recording them on a predetermined recording medium.

40. A recording apparatus in accordance with claim 39, wherein said predetermined condition is that more than a predetermined time has passed after said key-encrypting key was stored.

41. A recording apparatus in accordance with claim 39 or 40, wherein said relationship information is information related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents

encrypting means encrypts said digital data by using said contents key, a date/time when said key-encrypting key generating means generates said key-encrypting key, a date/time when said storing means stores said key-encrypting key, a date/time when said key encrypting means encrypts said contents key by using said key-encrypting key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium.

42. A recording apparatus in accordance with claim 39, wherein said predetermined condition is that the number of times said key-encrypting key is used at the time of reproducing said encrypted digital data exceeds a predetermined number of times.

43. A recording apparatus in accordance with one of claims 39 to 42, wherein a contents key generating means for generating said contents key is provided, and said contents encrypting means receives said contents key from said contents key generating means.

44. A recording apparatus in accordance with one of claims 39 to 42, wherein said contents encrypting means receives said contents key from a broadcasting station and uses said contents key.

45. A reproducing apparatus comprising:

a key-encrypting key obtaining means for receiving said

relationship information on said recording medium of said recording apparatus in accordance with one of claims 39 to 45, for specifying a key-encrypting key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information, and for retrieving and obtaining said key-encrypting key from said storing means of said recording means,

a key decrypting means for receiving said encrypted contents key corresponding to said encrypted digital data to be reproduced, from said predetermined recording medium, for receiving said key-encrypting key, and for decrypting said encrypted contents key by using said key-encrypting key, and

a contents decrypting means for decrypting said encrypted digital data by using said contents key from said key decrypting means.

46. A recording apparatus comprising:

a contents encrypting means for receiving digital data and a contents key for encrypting said digital data and for subjecting said digital data to first encrypting by using said contents key to generate encrypted digital data,

a key-encrypting key generating means for generating a key-encrypting key for subjecting said contents key to second encrypting,

a storing means for storing said key-encrypting key

generated by said key-encrypting key generating means,

a key encrypting means for encrypting said contents key by using said key-encrypting key,

a relationship information generating means for generating the relationship information between said encrypted digital data encrypted by using said contents key and said key-encrypting key obtained by encrypting said contents key, and

a recording means for receiving said encrypted digital data, said encrypted contents key and all or part of said relationship information and for recording them on a predetermined recording medium.

47. A recording apparatus in accordance with claim 46, wherein said relationship information is information related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents encrypting means encrypts said digital data by using said contents key, a date/time when said key-encrypting key generating means generates said key-encrypting key, a date/time when said storing means stores said key-encrypting key, a date/time when said key encrypting means encrypts said contents key by using said key-encrypting key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium.

48. A recording apparatus in accordance with claim 46 or 47, wherein a contents key generating means for generating said contents key is provided, and said contents encrypting means receives said contents key from said contents key generating means.

49. A recording apparatus in accordance with claim 46 or 47, wherein said contents encrypting means receives said contents key from a broadcasting station and uses said contents key.

50. A reproducing apparatus comprising:

a key-encrypting key obtaining means for receiving said relationship information on said recording medium of said recording apparatus in accordance with one of claims 46 to 49, for specifying a key-encrypting key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information, for judging whether said key-encrypting key satisfies a predetermined condition, and for taking out said key-encrypting key from said storing means of said recording apparatus when said condition is satisfied, or for not taking out said key-encrypting key from said storing means when said condition is not satisfied,

a key decrypting means for receiving said encrypted contents key corresponding to said encrypted digital data to be reproduced, from said predetermined recording medium, for receiving said key-encrypting key, and for decrypting

said encrypted contents key by using said key-encrypting key to restore said contents key, and

a contents decrypting means for decrypting said encrypted digital data by using said contents key from said key decrypting means.

Sub A6

51. A reproducing apparatus in accordance with claim 50, wherein said predetermined condition is that more than a predetermined time has passed after said key-encrypting key was stored in said storing means of said recording apparatus in accordance with one of claims 46 to 49.

52. A reproducing apparatus in accordance with claim 50, wherein said predetermined condition is that the number of times said key-encrypting key is used at the time of reproducing said encrypted digital data exceeds a predetermined number of times.

53. A recording apparatus comprising:

a contents key generating means for generating a contents key for encrypting digital data,

a storing means for storing said contents key generated by said contents key generating means and for deleting said contents key hereafter if said contents key satisfies a predetermined condition,

a contents encrypting means for encrypting said digital data by using said contents key,

a relationship information generating means for

generating the relationship information between said encrypted digital data encrypted by using said contents key and said contents key, and a recording means for receiving said encrypted digital data and all or part of said relationship information, and for recording them on a predetermined recording medium.

54. A recording apparatus in accordance with claim 53, wherein said predetermined condition is that more than a predetermined time has passed after said contents key was stored.

55. A recording apparatus in accordance with claim 53 or 54, wherein said relationship information is information related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents encrypting means encrypts said digital data by using said contents key, a date/time when said contents key generating means generates said contents key, a date/time when said storing means stores said contents key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium.

56. A recording apparatus in accordance with claim 53, wherein said predetermined condition is that the number of times said key-encrypting key is used at the time of reproducing said encrypted digital data exceeds a predetermined number of times.

57. A reproducing apparatus comprising:

a contents-key obtaining means for receiving said relationship information on said recording medium of said recording apparatus in accordance with one of claims 53 to 56, for specifying a contents key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information, and for retrieving and obtaining said contents key from said storing means of said recording means, and

a contents decrypting means for receiving said encrypted digital data from said predetermined recording medium, for receiving said contents key, and for decrypting said encrypted digital data by using said contents key.

58. A recording apparatus comprising:

a contents key generating means for generating a contents key for encrypting digital data,

a storing means for storing said contents key generated by said contents key generating means,

a contents encrypting means for encrypting said digital data by using said contents key to obtain encrypted digital data,

a relationship information generating means for generating the relationship information between said encrypted digital data encrypted by using said contents key and said contents key, and a recording means for receiving

said encrypted digital data and all or part of said relationship information, and for recording them on a predetermined recording medium.

59. A recording apparatus in accordance with claim 58, wherein said relationship information is information related by a date/time when said contents encrypting means receives said digital data, a date/time when said contents encrypting means contents-encrypts said digital data by using said contents key, a date/time when said contents key generating means generates said contents key, a date/time when said storing means stores said contents key, or a date/time when said recording means records said encrypted digital data on said predetermined recording medium.

60. A reproducing apparatus comprising:

a contents-key obtaining means for receiving said relationship information on said recording medium of said recording apparatus in accordance with claim 58 or 59, for specifying a contents key corresponding to said encrypted digital data to be reproduced on the basis of said relationship information, for judging whether said contents key satisfies a predetermined condition, and for taking out said contents key from said storing means of said recording apparatus when said condition is satisfied, or for not taking out said contents key from said storing means when said condition is not satisfied, and

a contents decrypting means for decrypting said encrypted digital data by using said contents key.

61. A reproducing apparatus in accordance with claim 60, wherein said predetermined condition is that more than a predetermined time has passed after said contents key was stored in said storing means of said recording apparatus in accordance with claim 58 or 59.

62. A reproducing apparatus in accordance with claim 60, wherein said predetermined condition is that the number of times said contents key is used at the time of reproducing said encrypted digital data exceeds a predetermined number of times.

63. A recording apparatus in accordance with one of claims 39 to 44, one of claim 46 or 49, one of claim 53 or 56, or one of claims 58 to 59, provided with a billing means for charging the amount of billing for recording said data at the time when said recording means records said encrypted digital data on said predetermined recording medium.

64. A recording apparatus in accordance with one of claims 39 to 44, one of claim 46 or 49, one of claim 53 or 56, or one of claims 58 to 59, wherein said predetermined recording medium is a video tape.

65. A recording apparatus in accordance with one of claims 39 to 44, one of claim 46 or 49, one of claim 53 or 56, or one of claims 58 to 59, wherein said predetermined

recording medium is a hard disk.

66. A program medium containing programs for attaining all or part of said components in accordance with one of claims 1 to 65.